I. Amendments to the Claims

Please amend the claims as follows with the following version of the claims in accordance with revised 37 CFR § 1.121.

1. (Canceled).

2. (Canceled).

3. (Canceled).

4. (Canceled).

5. (Canceled).

6. (Canceled).

7. (Canceled).

8. (Canceled).

9. (Canceled).

10. (Canceled).

11. (Canceled).

12. (Canceled).

13. (Canceled).

14. (Canceled).

15. (Canceled).

16. (Canceled).

17. (Canceled).

18. (Canceled).

19. (Canceled).

20. (Canceled).

21. (Canceled).

22. (Canceled).

23. (Canceled).

24. (Canceled).

25. (Canceled).

26. (Canceled).

27. (Canceled).

28. (Canceled).

29. (Canceled).

30. (Canceled).

31. (Canceled).

32. (Canceled).

33. (Canceled).

34. (Canceled).

35. (Canceled).

36. (Canceled).

37. (Canceled).

38. (Canceled).

39. (Canceled).

40. (Canceled).

41. (Canceled).

42. (Canceled).

43. (Canceled).

44. (Canceled).

45. (Canceled).

46. (Canceled).

47. (Canceled).

48. (New) A method for authenticating software modules that execute on a data processing system, the method comprising:

executing an instance of a first class on the data processing system;

in response to initiating a call from the instance of the first class to a second class, initiating an instantiation of the second class to create an instance of the second class;

while performing the instantiation of the second class, calling a class constructor for the second class;

during execution of the class constructor for the second class, determining a codebase for the first class;

during execution of the class constructor for the second class, attempting by the second class to verify a digital signature on the codebase for the first class;

in response to a successful verification of the digital signature on the codebase for the first class, successfully completing the instantiation of the second class;

in response to successfully completing the instantiation of the second class, determining by the first class a codebase for the second class;

in response to determining by the first class the codebase for the second class, attempting by the first class to verify a digital signature on the codebase for the second class; and

in response to a successful verification of the digital signature on the codebase for the second class, performing the call from the instance of the first class to the instance of the second class.

49. (New) The method of claim 48 further comprising:

in response to an unsuccessful verification of the digital signature on the codebase for the first class, unsuccessfully completing the instantiation of the second class.

50. (New) The method of claim 48 further comprising:

in response to an unsuccessful verification of the digital signature on the codebase for the second class, failing to perform the call from the instance of the first class to the instance of the second class.

51. (New) The method of claim 48 further comprising:

using a trusted digital certificate or a trusted public key embedded in the instance of the first class in attempting by the first class to verify a digital signature on the codebase for the second class.

52. (New) The method of claim 48 further comprising:

employing, in accordance with a source of randomness, a trusted digital certificate from multiple digital certificates embedded in the instance of the first class in attempting by the first class to verify a digital signature on the codebase for the second class, wherein the trusted digital certificate is obfuscated from viewing in the codebase for the first class.

53. (New) The method of claim 48 further comprising:

using a trusted digital certificate or a trusted public key embedded in the instance of the second class in attempting by the second class to verify a digital signature on the codebase for the first class.

54. (New) An apparatus for authenticating software modules that execute on a data processing system, the apparatus comprising:

means for executing an instance of a first class on the data processing system;

means for initiating an instantiation of the second class to create an instance of the second class in response to initiating a call from the instance of the first class to a second class;

means for calling a class constructor for the second class while performing the instantiation of the second class;

means for determining a codebase for the first class during execution of the class constructor for the second class;

means for attempting by the second class to verify a digital signature on the codebase for the first class during execution of the class constructor for the second class;

means for successfully completing the instantiation of the second class in response to a successful verification of the digital signature on the codebase for the first class;

means for determining by the first class a codebase for the second class in response to successfully completing the instantiation of the second class;

means for attempting by the first class to verify a digital signature on the codebase for the second class in response to determining by the first class the codebase for the second class; and

means for performing the call from the instance of the first class to the instance of the second class in response to a successful verification of the digital signature on the codebase for the second class.

55. (New) The apparatus of claim 54 further comprising:

means for unsuccessfully completing the instantiation of the second class in response to an unsuccessful verification of the digital signature on the codebase for the first class.

56. (New) The apparatus of claim 54 further comprising:

means for failing to perform the call from the instance of the first class to the instance of the second class in response to an unsuccessful verification of the digital signature on the codebase for the second class.

57. (New) The apparatus of claim 54 further comprising:

means for using a trusted digital certificate or a trusted public key embedded in the instance of the first class in attempting by the first class to verify a digital signature on the codebase for the second class.

58. (New) The apparatus of claim 54 further comprising:

means for employing, in accordance with a source of randomness, a trusted digital certificate from multiple digital certificates embedded in the instance of the first class in attempting by the first class to verify a digital signature on the codebase for the second class, wherein the trusted digital certificate is obfuscated from viewing in the codebase for the first class.

60. (New) The apparatus of claim 54 further comprising:

means for using a trusted digital certificate or a trusted public key embedded in the instance of the second class in attempting by the second class to verify a digital signature on the codebase for the first class.

61. (New) A computer program product on a computer readable medium for use in a data processing system for authenticating software modules that execute on the data processing system, the computer program product comprising:

instructions for executing an instance of a first class on the data processing system;

instructions for initiating an instantiation of the second class to create an instance of the second class in response to initiating a call from the instance of the first class to a second class;

instructions for calling a class constructor for the second class while performing the instantiation of the second class;

instructions for determining a codebase for the first class during execution of the class constructor for the second class;

instructions for attempting by the second class to verify a digital signature on the codebase for the first class during execution of the class constructor for the second class;

instructions for successfully completing the instantiation of the second class in response to a successful verification of the digital signature on the codebase for the first class;

instructions for determining by the first class a codebase for the second class in response to successfully completing the instantiation of the second class;

instructions for attempting by the first class to verify a digital signature on the codebase for the second class in response to determining by the first class the codebase for the second class; and

instructions for performing the call from the instance of the first class to the instance of the second class in response to a successful verification of the digital signature on the codebase for the second class.

62. (New) The computer program product of claim 61 further comprising:

instructions for unsuccessfully completing the instantiation of the second class in response to an unsuccessful verification of the digital signature on the codebase for the first class.

63. (New) The computer program product of claim 61 further comprising:

instructions for failing to perform the call from the instance of the first class to the instance of the second class in response to an unsuccessful verification of the digital signature on the codebase for the second class.

64. (New) The computer program product of claim 61 further comprising:

instructions for using a trusted digital certificate or a trusted public key embedded in the instance of the first class in attempting by the first class to verify a digital signature on the codebase for the second class.

65. (New) The computer program product of claim 61 further comprising:

instructions for employing, in accordance with a source of randomness, a trusted digital certificate from multiple digital certificates embedded in the instance of the first class in attempting by the first class to verify a digital signature on the codebase for the second class, wherein the trusted digital certificate is obfuscated from viewing in the codebase for the first class.

66. (New) The computer program product of claim 61 further comprising:

instructions for using a trusted digital certificate or a trusted public key embedded in the instance of the second class in attempting by the second class to verify a digital signature on the codebase for the first class.